Master, VSO, or designated representatives must sign the written DoS.

(2) For a vessel engaging in a vessel-to-vessel activity, prior to the activity, the respective Masters, VSOs, or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(c) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of the vessel-to-vessel activity. Upon the vessel-to-vessel activity and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective Masters, VSOs, or designated representatives must sign the written DoS.

(d) At MARSEC Levels 2 and 3, the Master, VSO, or designated representative of any manned vessel required to comply with this part must coordinate security needs and procedures, and agree upon the contents of the DoS for the period the vessel is at the facility. Upon the vessel's arrival to a facility and prior to any passenger embarkation or disembarkation or cargo transfer operation, the respective FSO and Master, VSO, or designated representatives must sign the written DoS.

(e) At MARSEC Levels 1 and 2, VSOs of vessels that frequently interface with the same facility may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for the specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond the level contained in the DoS, the continuing DoS becomes void and a new DoS must be signed and implemented in accordance with this section.

(g) The COTP may require at any time, at any MARSEC Level, any manned vessel subject to this part to implement a DoS with the VSO or FSO prior to any vessel-to-vessel activity or vessel-to-facility interface when he or she deems it necessary.

[USCG–2003–14749, 68 FR 39302, July 1, 2003, as amended at 68 FR 60514, Oct. 22, 2003]

§ 104.260 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated and maintained according to the manufacturer's recommendation.

(b) The results of testing completed under paragraph (a) of this section shall be recorded in accordance with § 104.235. Any deficiencies shall be promptly corrected.

(c) The Vessel Security Plan (VSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 104.265 Security measures for access control.

(a) *General.* The vessel owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on board;

(3) Control access to the vessel; and

(4) Prevent an unescorted individual from entering an area of the vessel that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

(b) The vessel owner or operator must ensure that the following are specified:

(1) The locations providing means of access to the vessel where access restrictions or prohibitions are applied for each Maritime Security (MARSEC) Level, including those points where TWIC access control provisions will be applied. ''Means of access'' include, but are not limited, to all:

(i) Access ladders;

(ii) Access gangways;

(iii) Access ramps;

(iv) Access doors, side scuttles, windows, and ports;

(v) Mooring lines and anchor chains; and

(vi) Cranes and hoisting gear;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC and procedures for escorting, in accordance with §101.515 of this subchapter; and

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level.

(c) The vessel owner or operator must ensure that a TWIC program is implemented as follows:

(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with §101.514 of this subchapter. Inspection must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the vessel and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than seven consecutive calendar days provided that:

(i) The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f);

(ii) The individual can present another identification credential that meets the requirements of §101.515 of this subchapter; and

(iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.

(3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside a secure area.

(4) With the exception of persons granted access according to paragraph (2) of this section, all persons granted unescorted access to secure areas of the vessel must be able to produce his or her TWIC upon request.

(5) There must be disciplinary measures in place to prevent fraud and abuse.

(6) The vessel's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of facilities or other transportation conveyances that interface with the vessel.

(d) If the vessel owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.

(e) The vessel owner or operator must establish in the approved VSP the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis.

(f) *MARSEC Level 1.* The vessel owner or operator must ensure security measures in this paragraph are implemented to:

(1) Employ TWIC as set out in paragraph (c) of this section.

(2) Screen persons, baggage (including carry-on items), personal effects, and vehicles for dangerous substances and devices at the rate specified in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(3) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Boarding the vessel is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to board;

(4) Check the identification of any person not holding a TWIC and seeking to board the vessel, including vessel

passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check includes confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section.

(5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of vessel personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(6) Deter unauthorized access to the vessel;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access;

(9) Provide a designated area on board, within the secure area, or in liaison with a facility, for conducting inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicle's contents;

(10) Ensure vessel personnel are not subjected to screening, of the person or of personal effects, by other vessel personnel, unless security clearly requires it;

(11) Conduct screening in a way that takes into full account individual human rights and preserves the individual's basic human dignity;

(12) Ensure the screening of all unaccompanied baggage;

(13) Ensure checked persons and their personal effects are segregated from unchecked persons and their personal effects;

(14) Ensure embarking passengers are segregated from disembarking passengers;

(15) Ensure, in liaison with the facility, a defined percentage of vehicles to be loaded aboard passenger vessels are screened prior to loading at the rate specified in the approved VSP;

(16) Ensure, in liaison with the facility, all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading; and

(17) Respond to the presence of unauthorized persons on board, including repelling unauthorized boarders.

(g) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people, personal effects, and vehicles being embarked or loaded onto the vessel as specified for MARSEC Level 2 in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to patrol deck areas during periods of reduced vessel operations to deter unauthorized access;

(4) Limiting the number of access points to the vessel by closing and securing some access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the vessel, which may include, in liaison with the facility, providing boat patrols; and

(7) Establishing a restricted area on the shore side of the vessel, in close cooperation with the facility.

(h) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. The additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively, for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage on board;

(3) Being prepared to cooperate with responders and facilities;

(4) Limiting access to the vessel to a single, controlled access point;

(5) Granting access to only those responding to the security incident or threat thereof;

(6) Suspending embarkation and/or disembarkation of personnel;

(7) Suspending cargo operations;

(8) Evacuating the vessel;

(9) Moving the vessel; or

(10) Preparing for a full or partial search of the vessel.

[USCG–2006–24196, 72 FR 3580, Jan. 25, 2007]

§ 104.267 Security measures for newly hired employees.

(a) Newly-hired vessel employees may be granted entry to secure areas of the vessel for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the vessel. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired vessel employees may be granted the access provided for in paragraph (a) of this section only if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The vessel owner or operator or Vessel Security Officer (VSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The vessel owner or operator or the VSO enters the following information on the new hire into the Coast Guard's Homeport website (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment;

(3) The new hire presents an identification credential that meets the requirements of §101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the vessel owner or operator or VSO have not been informed by the cognizant COTP that the new hire poses a security threat; and

(5) There would be an adverse impact to vessel operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a Company Security Officer (CSO) or VSO, or any individual being hired to perform vessel security duties.

(d) The new hire may not begin working on board the vessel under the provisions of this section until the owner, operator, or VSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

[USCG–2006–24196, 72 FR 3581, Jan. 25, 2007]

§ 104.270 Security measures for restricted areas.

(a) *General.* The vessel owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be on board;

(3) Protect the vessel;

(4) Protect sensitive security areas within the vessel;